CLAIMS:

1.   (Currently amended) A method, in a data processing system, for providing a system administrator with a view of a plurality of applications accessible by a user, comprising:

receiving, in the data processing system, in response to a coupling of a separate hardware security device to the data processing system, credential information comprising user names and associated passwords for each application of the plurality of applications that the user uses, from the separate hardware security device into an authentication credential container associated with the user;

identifying, by the data processing system, the plurality of applications accessible by the user by examining the authentication credential container associated with the user;

generating, by the data processing system, a view of the plurality of applications accessible by the user, wherein the view is a consolidated user directory that contains user authentication information across the plurality of applications; and

displaying, by the data processing system, the view to the administrator.

2.   (Canceled)

3.   (Previously presented) The method of claim 1 further comprising removing access to an application from the plurality of the applications by utilizing the view of the plurality of the applications accessible by the user.

4.   (Original) The method of claim 1 further comprising:

creating a user account for a new application to be accessible by the user utilizing the generated view; and

injecting authentication information of the user account into the authentication credential container of the user.

5.   (Original) The method of claim 4 wherein the authentication credential container is stored at a server.

6.   (Original) The method of claim 3 wherein the removing is performed automatically.

7.   (Previously presented) The method of claim 4 wherein the creating the user account is performed either automatically or manually by an administrator.

8.   (Canceled)

9.   (Previously presented) The method of claim 4 wherein the authentication information is injected into the separate hardware security device.

10.   (Previously presented) The method of claim 1 further comprising removing individual user directories for each application of the plurality of the applications accessible by the user.

11-16. (Canceled)

17.   (Currently amended) A method, in a data processing system, for providing a system administrator with a list of a plurality of applications accessible by a user together with any user names and passwords used in connection with those applications, comprising:

        receiving, in the data processing system, in response to a coupling of a separate hardware security device to the data processing system, credential information comprising user names and associated passwords for each application of a plurality of applications that the user uses, from the separate hardware security device into an authentication credential container associated with the user;

        identifying, by the data processing system, the plurality of applications accessible by the user and [[any]] user names and passwords used in connection with the plurality of applications by examining an authentication credential container associated with the user;

generating, by the data processing system, a list of the plurality of applications accessible by the user together with any user names and passwords used in connection with the plurality of applications; and

displaying, by the data processing system, the list to the administrator.

18-20. (Canceled)

21.   (Previously presented) The method of claim 1, wherein the view comprises:
a list of keys employed by the user, wherein each entry in the list corresponds to a different key employed by the user, and wherein each entry identifies a type of the corresponding key and a serial number of the corresponding key.

22.   (Previously presented) The method of claim 1, wherein the view comprises:
a profile of the user detailing a role of the user, a name of the user, contact information for the user, and employment information for the user.

23.   (Previously presented) The method of claim 1, wherein the view comprises:
a list of certificate-enabled applications accessible by the user, wherein each entry in the list corresponds to a different certificate-enabled application, and wherein each entry identifies a user name of the user and a last login attempt of the user for the corresponding certificate-enabled application.

24.   (Previously presented) The method of claim 1, wherein the view comprises:
a list of enterprise applications accessible by the user, wherein each entry in the list corresponds to a different enterprise application, and wherein each entry identifies a user name of the user and a last login attempt of the user for the corresponding enterprise application.

25.   (Previously presented) The method of claim 1, wherein the view comprises:
a list of personal applications accessible by the user, wherein each entry in the list corresponds to a different personal application, and wherein each entry identifies a number of accounts connected to the corresponding personal application.

26.   (Previously presented) The method of claim 22, wherein the view comprises:
user selectable graphical user interface elements for invoking a function to update the profile and for invoking a function to reset the profile.

27.   (Previously presented) The method of claim 23, wherein the view comprises:
a user selectable graphical user interface element for invoking a function to delete a user name of the user from the list of certificate-enabled applications.

28.   (Currently amended) A computer program product comprising a computer recordable medium having a computer readable program recorded thereon, wherein the computer readable program, when executed on a data processing system, causes the data processing system to:
receive, in response to a coupling of a separate hardware security device to the data processing system, credential information comprising user names and associated passwords for each application of the plurality of applications that the user uses, from the separate hardware security device into an authentication credential container associated with the user;
identify the plurality of applications accessible by the user by examining the authentication credential container associated with the user;
generate a view of the plurality of applications accessible by the user, wherein the view is a consolidated user directory that contains user authentication information across the plurality of applications; and
display the view to the administrator.

29.   (Previously presented) The computer program product of claim 28, wherein the computer readable program further causes the data processing system to remove access to

an application from the plurality of the applications by utilizing the view of the plurality of the applications accessible by the user.

30.   (Previously presented) The computer program product of claim 28, wherein the computer readable program further causes the data processing system to:

create a user account for a new application to be accessible by the user utilizing the generated view; and

inject authentication information of the user account into the authentication credential container of the user.

31.   (Previously presented) The computer program product of claim 28, wherein the view comprises at least one of:

a list of certificate-enabled applications accessible by the user, wherein each entry in the list corresponds to a different certificate-enabled application, and wherein each entry identifies a user name of the user and a last login attempt of the user for the corresponding certificate-enabled application;

a list of enterprise applications accessible by the user, wherein each entry in the list corresponds to a different enterprise application, and wherein each entry identifies a user name of the user and a last login attempt of the user for the corresponding enterprise application;

a list of personal applications accessible by the user, wherein each entry in the list corresponds to a different personal application, and wherein each entry identifies a number of accounts connected to the corresponding personal application;

user selectable graphical user interface elements for invoking a function to update the profile and for invoking a function to reset the profile; or

a user selectable graphical user interface element for invoking a function to delete a user name of the user from the list of certificate-enabled applications.